UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/975,815	10/11/2001	Neal A. Krawetz	10019968-1	9182

7590 05/17/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
05/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/975,815	KRAWETZ, NEAL A.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 December 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on 12/5/2006, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below.

Response to Arguments

2. In response to communications filed on 12/5/2006, the following claims 1-34 are presented for examination.

2.1 Applicant's remarks, pages 4-19, filed on 12/5/2006, with respect to the rejection of claims 1-34 have been fully considered but they are moot in view of a new ground of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,764,772 to **Kaufman et al** *(Applicant's Disclosure)* in view of US Patent 6,728,378 to **Garib**.

As per claim 1, Kaufman et al substantially teaches a method for secure data transmission, comprising:

generating a character string (bit string referred to as salt) at a sender (see column 7, lines 42-50);

generating a hash key (hash) using the character string (salt) and a private key (secret key) (see column 7, lines 30-50 and column 12, lines 14-15);

and transmitting an identification key associated with the sender (see column 11, lines 45-50), the character string (see col. 8, lines 51-57), and the encrypted data (encrypted message) from the sender to a recipient (see col. 8, lines 51-57).

Kaufman et al discloses encrypting the message (data) using a secret key that is part of the hash, and suggests that any well-known hash functions may be used, but does not explicitly disclose encrypting the message (data) using the hash. **Garib** in an analogous art teaches a secret key messaging wherein a message hash value is generated and both the message (data) and the message hash value are encrypted using a password hash value as the secret key (see column 12, lines 21-26). **Garib** discloses several advantages in using a hash as a secret key for encryption of the message such as ensuring the integrity of the message as well as the confidentiality of the message (see column 3, lines 38-52). In addition the secret key does not have to be sent to the recipient as the recipient can generate it by applying the hashing algorithm. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the features of **Kaufman et al** of using a salt (string) concatenated with a secret key to enforce the security of a secret key (see column 7, lines 44-50) with the features of encrypting the message (data) using a hash as a key as suggested by **Garib**. One of ordinary skill in the art would have recognized some of the advantages of ensuring the integrity of the message as well as the confidentiality of the message as suggested by **Garib** (see column 3, lines 38-52).

As per claim 2, the combination of **Kaufman et al** and **Garib** discloses the limitation of wherein generating the hash key comprises hashing the character string with the private key (see **Kaufman et al**, column 7, lines 44-50 and fig.1, reference number 14).

As per claim 3, the combination of **Kaufman et al** and **Garib** discloses generating a signature using the hash key and the data, and transmitting the signature to the recipient (see **Kaufman et al**, column 7, lines 44-50 and column 4, lines 41-55), see also (**Garib** column 3, lines 47-52 and column 4, lines 62-67).

As per claim 4, the combination of **Kaufman et al** and **Garib** discloses wherein generating a character string comprises randomly generating the character string (see **Kaufman et al**, column 7, lines 45-47).

As per claim 5, the combination of **Kaufman et al** and **Garib** discloses determining the private key at the recipient using the identification key; and decrypting the encrypted data at the recipient using the private key and the character string (see **Kaufman et al**, column 10, line 64 through column 11, line 2 and column 11, lines 45-61 suggesting using identification of the sender as part of the encrypted information and suggesting using other information such as identification of the sender in the secret field).

As per claim 6, the combination of **Kaufman et al** and **Garib** discloses the limitation of wherein the recipient is adapted to access a relational database associating the identification key with the private key (see **Kaufman et al**, column 8, lines 13-20). **Kaufman et al**, column 10, line 64 through column 11, line 2 and column 11, lines 45-61 suggests using identification of the

sender as part of the encrypted information and suggests using other information such as identification of the sender in the secret field.

As per claim 7, the combination of **Kaufman et al** and **Garib** discloses determining the private key at the recipient using the identification key; **Kaufman et al**, column 10, line 64 through column 11, line 2 and column 11, lines 45-61 suggests using identification of the sender as part of the encrypted information and suggests using other information such as identification of the sender in the secret field.

determining the hash key at the recipient using the private key and the character string (see **Kaufman et al**, column 8, lines 58-64); and

decrypting the encrypted data using the hash key (see **Garib**, column 8, lines 40-42). **Claim 7** is also rejected on the same rationale as the rejection of claim 1.

As per claim 8, the combination of **Kaufman et al** and **Garib** discloses wherein determining the hash key comprises hashing the private key with the character string (see **Kaufman et al**, column 8, lines 58-64).

As per claim 9, the combination of **Kaufman et al** and **Garib** discloses generating a first signature by the sender using the hash key and the data and transmitting the first signature to the recipient (see **Kaufman et al**, column 7, lines 44-50 and column 4, lines 41-55), see also (**Garib** column 3, lines 47-52 and column 4, lines 62-67); and

the recipient adapted to determine the hash key for decrypting the data and compare the first signature to a second signature generated by the recipient using the hash key and the decrypted data (see **Garib**, column 9, lines 1-22 and column 10, lines 15-40). **Claim 9** is also rejected on the same rationale as the rejection of claim 1.

As per claim 10, the combination of **Kaufman et al** and **Roberts** discloses the limitation of generating a signature using the hash key and the data and transmitting the signature to the recipient (see **Kaufman et al**, column 7, lines 44-50 and column 4, lines 41-55), see also (**Garib** column 3, lines 47-52 and column 4, lines 62-67);

determining the private key at the recipient using the identification key (see **Kaufman et al**, column 10, line 64 through column 11, line 2 and column 11, lines 45-61 suggesting using identification of the sender as part of the encrypted information and suggesting using other information such as identification of the sender in the secret field);

determining the hash key at the recipient using the private key and the character string (see **Kaufman et al**, column 8, lines 58-64);

decrypting the encrypted data at the recipient using the hash key (see **Garib**, column 8, lines 40-42); and

verifying the signature at the recipient using the hash key and the decrypted data (see **Kaufman et al**, column 8, line 50 through column 9, line 7), (see **Garib**, column 8, lines 40-42). **Claim 10** is also rejected on the same rationale as the rejection of claim 1.

As per claim 11, Kaufman et al substantially teaches a method for secure data transmission, comprising:

generating a character string (bit string referred to as salt) at a sender (see column 7, lines 42-50)

receiving a character string from a sender (see column 8, lines 51-57);

receiving an identification key from the sender (see column 11, lines 45-50);

receiving encrypted data from the sender (see column 8, lines 20-27 and lines 51-57);

determining a private key associated with the sender using the identification key (see **Kaufman et al**, column 10, line 64 through column 11, line 2 and column 11, lines 45-61 suggesting using identification of the sender as part of the encrypted information and suggesting using other information such as identification of the sender in the secret field);

and decrypting the encrypted data using the private key and the character string (see column 11, lines 7-21), **Kaufman et al** discloses herein that the salt (string) is also used in decrypting the message with a secret key which meets the recitation of decrypting the encrypted data using the private key and the character string. See also column 13, line 38 through column 14, line 20). **Kaufman et al** discloses does not explicitly disclose encrypting the message (data) using the secret key and the salt (hash) which is not really required by the claim limitation as per Examiner's interpretation above. To meet the claim interpretation encrypting/decrypting the message (data) using the secret key and the salt (hash), **Garib** in an analogous art teaches a secret key messaging wherein a message hash value is generated and both the message (data) and the message hash value are encrypted using a password hash value as the secret key (see column 12, lines 21-26). **Garib** discloses several advantages in using a hash as a secret key for encryption of the message such as ensuring the integrity of the message as well as the

confidentiality of the message (see column 3, lines 38-52). In addition the secret key does not have to be sent to the recipient as the recipient can generate it by applying the hashing algorithm. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the features of **Kaufman et al** of using a salt (string) concatenated with a secret key to enforce the security of a secret key (see column 7, lines 44-50) with the features of encrypting the message (data) using a hash as a key as suggested by **Garib**. One of ordinary skill in the art would have recognized some of the advantages of ensuring the integrity of the message as well as the confidentiality of the message as suggested by **Garib** (see column 3, lines 38-52).

As per claim 12, the combination of **Kaufman et al** and **Garib** discloses determining a hash key using the character string and the private key, (see **Kaufman et al**, column 8, lines 58-64); and

decrypting the encrypted data using the hash key (see **Garib**, column 8, lines 40-42). **Claim 12** is also rejected on the same rationale as the rejection of claim 11.

As per claim 13, the combination of **Kaufman et al** and **Garib** discloses the limitation of wherein the recipient is adapted to access a relational database associating the identification key with the private key (see **Kaufman et al**, column 8, lines 13-20). **Kaufman et al**, column 10, line 64 through column 11, line 2 and column 11, lines 45-61 suggests using identification of the sender as part of the encrypted information and suggests using other information such as identification of the sender in the secret field.

As per claim 14, the combination of **Kaufman et al** and **Garib** discloses wherein generating a character string comprises randomly generating the character string (see **Kaufman et al**, column 7, lines 45-47).

As per claim 15, the combination of **Kaufman et al** and **Garib** discloses hashing the character string with the private key to generate a hash key (see **Kaufman et al**, column 8, lines 58-64); and wherein decrypting the encrypted data comprises decrypting the encrypted data using the hash key (see **Garib**, column 8, lines 40-42). **Claim 15** is also rejected on the same rationale as the rejection of claim 11.

As per claim 16, the combination of **Kaufman et al** and **Garib** discloses receiving a signature from the sender (see **Kaufman et al**, column 7, lines 44-50 and column 4, lines 41-55), see also (**Garib** column 3, lines 47-52 and column 4, lines 62-67); and

verifying the signature using the decrypted data, the private key, and the character string (see **Kaufman et al**, column 8, line 50 through column 9, line 7) (see **Garib**, column 9, lines 1-22 and column 10, lines 15-40). **Claim 16** is also rejected on the same rationale as the rejection of claim 11.

As per claim 17, the combination of **Kaufman et al** and **Garib** discloses receiving a signature from the sender (see **Kaufman et al**, column 7, lines 44-50 and column 4, lines 41-55), see also (**Garib** column 3, lines 47-52 and column 4, lines 62-67); determining a hash key at the

recipient using the private key and the character string (see **Kaufman et al**, column 8, lines 58-64); and

verifying the signature using the hash key and the decrypted data (see **Kaufman et al**, column 8, line 50 through column 9, line 7) (see **Garib**, column 9, lines 1-22 and column 10, lines 15-40). **Claim 17** is also rejected on the same rationale as the rejection of claim 11.

As per claim 18, the combination of **Kaufman et al** and **Garib** discloses receiving a signature from the sender (see **Kaufman et al**, column 7, lines 44-50 and column 4, lines 41-55), see also (**Garib** column 3, lines 47-52 and column 4, lines 62-67); determining a hash key at the recipient using the private key and the character string (see **Kaufman et al**, column 8, lines 58-64); and

generating a second signature using the hash key and the decrypted data; and

comparing the first signature to the second signature (see **Kaufman et al**, column 8, line 50 through column 9, line 7) (see **Garib**, column 9, lines 1-22 and column 10, lines 15-40). **Claim 17** is also rejected on the same rationale as the rejection of claim 11.

As per claim 19, Kaufman et al substantially teaches a system for secure data transmission, (see column 11, lines 51-56) comprising: (computer readable medium executed by a computer) for performing the invention (see for example claims 15-16), that meets the recitation of a processor; a memory coupled to the processor; a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string (see column 7, lines 42-50);

a hashing engine stored in the memory and executable by the processor, the hashing

engine adapted to generate a hash key (hash) using the character string (salt) and a private key (secret key) (see column 7, lines 30-50 and column 12, lines 14-15);

wherein the processor is adapted to transmit the encrypted data (encrypted message) and the character string to a recipient (see col. 8, lines 51-57); and **Kaufman et al** discloses encrypting the message (data) using a secret key that is part of the hash, and suggests that any well-known hash functions may be used, but does not explicitly disclose encrypting the message (data) using the hash. **Garib** in an analogous art teaches a secret key messaging wherein a message hash value is generated and both the message (data) and the message hash value are encrypted using a password hash value as the secret key (see column 12, lines 21-26). **Garib** discloses several advantages in using a hash as a secret key for encryption of the message such as ensuring the integrity of the message as well as the confidentiality of the message (see column 3, lines 38-52). In addition the secret key does not have to be sent to the recipient as the recipient can generate it by applying the hashing algorithm. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the features of **Kaufman et al** of using a salt (string) concatenated with a secret key to enforce the security of a secret key (see column 7, lines 44-50) with the features of encrypting the message (data) using a hash as a key as suggested by **Garib**. One of ordinary skill in the art would have recognized some of the advantages of ensuring the integrity of the message as well as the confidentiality of the message as suggested by **Garib** (see column 3, lines 38-52).

As per claim 20, the combination of **Kaufman et al** and **Garib** discloses comprising a signature engine (hash algorithm) stored in the memory and executable by the processor, the

signature engine adapted to generate a signature using the hash key and the data, the processor further adapted to transmit the signature to the recipient (see **Kaufman et al**, column 7, lines 44-50 and column 4, lines 41-55), see also (**Garib** column 3, lines 47-52 and column 4, lines 62-67).

As per claim 21, the combination of **Kaufman et al** and **Garib** discloses wherein the recipient is adapted to decrypt the encrypted data and verify the signature using the decrypted data (see **Kaufman et al**, column 8, line 50 through column 9, line 7) (see **Garib**, column 9, lines 1-22 and column 10, lines 15-40). **Claim 16** is also rejected on the same rationale as the rejection of claim 11.

As per claim 22, the combination of **Kaufman et al** and **Garib** discloses wherein the hashing engine is adapted to hash the character string with the private key to generate the hash key (see **Kaufman et al**, column 8, lines 58-64).

As per claim 23, the combination of **Kaufman et al** and **Garib** discloses wherein the string generator is adapted to randomly generate the character string. (see **Kaufman et al**, column 7, lines 45-47).

As per claim 24, the combination of **Kaufman et al** and **Garib** discloses wherein the recipient is adapted to decrypt the encrypted data using the identification key and the character string. (see **Kaufman et al**, column 8, lines 13-20). **Kaufman et al**, column 10, line 64 through column 11, line 2 and column 11, lines 45-61 suggests using identification of the sender as part of the

encrypted information and suggests using other information such as identification of the sender in the secret field. **Claim 24** is also rejected on the same rationale as the rejection of claim 19.

As per claim 25, the combination of **Kaufman et al** and **Garib** discloses wherein the recipient is adapted to determine the hash key using the identification key and the character string, (see **Kaufman et al**, column 8, lines 58-64); **Kaufman et al**, column 10, line 64 through column 11, line 2 and column 11, lines 45-61 suggests using identification of the sender as part of the encrypted information and suggests using other information such as identification of the sender in the secret field;

and decrypting the encrypted data using the hash key (see **Garib**, column 8, lines 40-42). **Claim 25** is also rejected on the same rationale as the rejection of claim 19.

As per claim 26, the combination of **Kaufman et al** and **Garib** discloses the limitation of wherein the recipient is adapted to access a relational database associating the identification key with the private key (see **Kaufman et al**, column 8, lines 13-20). **Kaufman et al**, column 10, line 64 through column 11, line 2 and column 11, lines 45-61 suggests using identification of the sender as part of the encrypted information and suggests using other information such as identification of the sender in the secret field.

As per claim 27, Kaufman et al substantially teaches a system for secure data transmission, (see column 11, lines 51-56) comprising: (computer readable medium executed by

a computer) for performing the invention (see for example claims 15-16), that meets the recitation of a processor adapted to receive encrypted data, an identification key, and a character string from a sender recipient (see col. 8, lines 51-57); a processor; a memory coupled to the processor; a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string (see column 7, lines 42-50); a relational database stored in the memory and accessible by the processor, the relational database relating the identification key to a private key (see **Kaufman et al**, column 8, lines 13-20). **Kaufman et al**, column 10, line 64 through column 11, line 2 and column 11, lines 45-61 suggests using identification of the sender as part of the encrypted information and suggests using other information such as identification of the sender in the secret field. Examiner takes official notice that it is well known that hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value. It is also used in many encryption algorithms;

a decryption engine stored in the memory and executable by the processor, the decryption engine adapted to decrypt the encrypted data using the private key and the character string (see column 11, lines 7-21), **Kaufman et al** discloses herein that the salt (string) is also used in decrypting the message with a secret key which meets the recitation of decrypting the encrypted data using the private key and the character string. See also column 13, line 38 through column 14, line 20). **Kaufman et al** discloses does not explicitly disclose encrypting the message (data) using the secret key and the salt (hash) which is not really required by the claim limitation as per Examiner's interpretation above. To meet the claim interpretation encrypting/decrypting the message (data) using the secret key and the salt (hash), **Garib** in an

analogous art teaches a secret key messaging wherein a message hash value is generated and both the message (data) and the message hash value are encrypted using a password hash value as the secret key (see column 12, lines 21-26). **Garib** discloses several advantages in using a hash as a secret key for encryption of the message such as ensuring the integrity of the message as well as the confidentiality of the message (see column 3, lines 38-52). In addition the secret key does not have to be sent to the recipient as the recipient can generate it by applying the hashing algorithm. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the features of **Kaufman et al** of using a salt (string) concatenated with a secret key to enforce the security of a secret key (see column 7, lines 44-50) with the features of encrypting the message (data) using a hash as a key as suggested by **Garib**. One of ordinary skill in the art would have recognized some of the advantages of ensuring the integrity of the message as well as the confidentiality of the message as suggested by **Garib** (see column 3, lines 38-52).

As per claim 28, the combination of **Kaufman et al** and **Garib** discloses a hashing engine stored in the memory and executable by the processor, the hashing engine adapted generate a hash key using the private key and the character string (see **Kaufman et al**, column 8, lines 58-64); and

decrypting the encrypted data using the hash key (see **Garib**, column 8, lines 40-42). **Claim 28** is also rejected on the same rationale as the rejection of claim 27.

As per claim 29, the combination of **Kaufman et al** and **Garib** discloses comprising a signature engine (hash algorithm) stored in the memory and executable by the processor, the signature engine adapted to verify a signature received from the sender using the private key and the character string. (see **Kaufman et al**, column 7, lines 44-50 and column 4, lines 41-55), see also (**Garib** column 3, lines 47-52 and column 4, lines 62-67).

As per claim 30, the combination of **Kaufman et al** and **Garib** discloses a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the private key and the character string (see **Kaufman et al**, column 8, lines 58-64); and

a signature engine stored in the memory and executable by the processor, the signature engine adapted to verify a signature received from the sender using the hash key and the decrypted data (see **Garib**, column 9, lines 1-22 and column 10, lines 15-40). **Claim 30** is also rejected on the same rationale as the rejection of claim 27.

As per claim 31, the combination of **Kaufman et al** and **Garib** discloses a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to hash the character string with the private key to generate a hash key (see **Kaufman et al**, column 8, lines 58-64); and the decryption engine adapted to decrypt the encrypted data using the hash key (see **Garib**, column 9, lines 1-22 and column 10, lines 15-40). **Claim 31** is also rejected on the same rationale as the rejection of claim 27.

As per claim 32, the combination of **Kaufman et al** and **Garib** discloses a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string (see **Kaufman et al,** column 7, lines 42-50), and wherein the decryption engine is further adapted to encrypt data for transmitting to the sender using the character string and the private key (see **Garib,** column 12, lines 21-26). **Claim 32** is also rejected on the same rationale as the rejection of claim 27.

As per claim 33, the combination of **Kaufman et al** and **Garib** discloses a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string (see **Kaufman et al,** column 7, lines 42-50); a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the private key and the character string (see **Kaufman et al**, column 8, lines 58-64); and wherein the decryption engine is further adapted to encrypt data for transmitting to the sender using the character string and the private key (see **Garib,** column 12, lines 21-26). **Claim 33** is also rejected on the same rationale as the rejection of claim 27.

As per claim 34, the combination of **Kaufman et al** and **Garib** discloses a signature engine stored in the memory and executable by the processor, the signature engine adapted to generate a first signature using the decrypted data and compare the first signature to a second signature received from the sender (see **Kaufman et al**, column 7, lines 44-50 and column 4, lines 41-55), see also (**Garib** column 3, lines 47-52 and column 4, lines 62-67).). **Claim 34** is also rejected on the same rationale as the rejection of claim 27.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (see PTO-form 892).

4.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cc

Carl Colin
Patent Examiner
May 13, 2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER